

“UIB to be or NOT to be”



Ernst Selmer

Security research at the Selmer Center
Department of Informatics
University of Bergen

Outline

- Introduction
- Research projects
- Recent Completed Projects
- Recent Publication & Activities
- The Selmer Center In 2010



Ernst S. Selmer (1920-2006)



- Named after professor Ernst S. Selmer
- Professor in Mathematics UiB 1957-1990
- Pioneer in coding and cryptology in Norway
 - Cryptographer during WW2
 - Consultant for government
 - Crypto (Hagelin)
 - Coding (Personnum.)

The Selmer Center



- **Research center in secure communication**
- **Present staff (25 members)**
 - 6 professors
 - 7 post-docs/researchers
 - 12 PhD students
- **Research areas**
 - Coding (Reliable communication during transmission and storage of data)
 - Cryptography (Cryptographic techniques, Secure communication)
 - Data Security (NoWires group)
- **Active publication records**
 - > 300 journal/conference publications since 2004
 - 50% has an international co-author

Outline

- Introduction
- Research projects
- Recent Completed Projects
- Recent Publication & Activities
- The Selmer Center In 2010



Research Projects-Security



EU projects

- **Net-on-Demand:** Lightweight cryptography, 2006-2009
 - Collaboration with University of Leeds, University of Brest, NERA etc
- **ECRYPT II:** Network of Excellence in Cryptography, 2008-2011
- **NILNET:** Collaboration with Slovakia in cryptography, 2008-2010

NFR projects

- **ICC:RASC** Inductive coupled channels: Reliable and secure communication (VERDIKT program), 2007-2010
- **SETA:** Sequences and their applications (FRITEK), 2007-2010
- **NISNet:** Resource Network Information Theory, 2007-2010
- **QIT:** Quantum Information Theory, 2008-2011
- **SEC:** Studies in error detecting codes, 2009-2012

Research in cryptography



- Stream ciphers including phase 3 candidate **POMARANCH** in eSTREAM project (Helleseeth, Kholosha, Sondre)
- Hash functions (Mehdi, Tor Erling)
- Solving nonlinear equations (Igor, Torstein)
- Lightweight cryptography (Security in RFID and sensor networks) (Reza)
- Cryptanalysis of block cipher (Håvard)



NoWires-Data security

- Headed by Prof. Kjell Hole
- does applied and basic security research.
- main focus is on understanding security and privacy risks associated with large national and international information systems.
- 5 PhD students graduated in 2006-2008
- External active in the media > 200 times in media during the last three years (The attacks on Internet banks)
- Lately, the group has been particularly interested in evaluating the risks associated with large identity systems and electronic voting systems



No Wires-Ongoing research projects

- Risk assessment of Norway's new electronic voting system ("E-valg 2011")
- Risk assessment of UiB's electronic voting system
- Evaluation of new authentication techniques using mobile phones
- Design rules to avoid catastrophic risks in large national information systems

Outline

- Introduction
- Research projects
- Recent Completed Projects
- Recent Publication & Activities
- The Selmer Center In 2010



Recent Completed Projects



NEWCOM: EU Network of Excellence (Mobile communication) (2003-2007)

ECRYPT: EU Network of Excellence (Mobile communication) (2003-2007)

RASC: Reliable And Secure Communication (2001-2006)

ACT: Advanced Cryptographic Techniques (2003-2007)

ALBRICC: A Little bit of Basic Research In Coding and Crypto (2005-2008)

SEC: Studies in Error-correcting Codes (2004-2008)

SWAP: Secure Wireless Applications (2005-2008)

OWL: Optimization techniques in Wireless Networks (2006-2009)

INTERRASC: International collaborations in Reliable and Secure Communication(2006-2009)

Outline

- Introduction
- Research projects
- Recent Completed Projects
- **Recent Publication & Activities**
- The Selmer Center In 2010





Recent Publication Activities

	2002	2003	2004	2005	2006	2007	2008	2009	Sum
Book/Ed/Chap.	3	1	1	2	2	3	3	2	17
Journal pap.	11	19	34	15	20	15	20	17	151
Conf. Proc.	13	16	14	24	20	28	32	17	164
Other publ.	6	8	9	6	2	2	0	2	35

“Publication list for 2009 is incomplete”

During 2001-2005: 101 journal papers and **84** papers in conference proceedings.
Of these **114** had a foreign co-author outside the Selmer Center (60%).

During 2006-2007: 55 journal papers and **80** conference paper. Of these **52** had
a foreign co-author outside the Selmer Center (40%).

Conference Activities



- **In 2009**

- Winter school in Information Security
 - Finse 3-8 May, (30 Participants), 2009
- Workshop in Coding and Cryptography (WCC09)
 - Ullensvang, May 10-15, (90 Participants), 2009
 - Organized in collaboration with INRIA, France
 - Held bi-annually alternating between Paris and Bergen
 - Next WCC will be organized in France in 2011

- **Before 2009**

- 8 International Conferences
- 2 National Conferences

Outline

- Introduction
- Research projects
- Recent Completed Projects
- Recent Publication & Activities
- **The Selmer Center In 2010**



Selmer Center In 2010



■ Staff 2010 (Total 22 Members)

- Professors (6) - Helleseth/Hole/Kløve/Parker/Semaev/Ytrehus
- Post-docs (4) - Budaghyan/Danielsen/Naydenova
- Researchers (3) - Kholosha/Raddum/Rosnes
- PhD students (9)

■ Conference Activities in 2010

- Winter school in Information Security (2010)

Finse 25-30 April, 2010, 30 Participants



Thank you for your attention

